IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
-vs-	)	Case No. 18 CR 789
	)	
DENY MITROVICH,	)	Chicago, Illinois
	)	February 24, 2020
Defendant.	)	10:00 a.m.

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE GARY FEINERMAN

APPEARANCES:

For the Government:
HON. JOHN R. LAUSCH, JR.
UNITED STATES ATTORNEY
BY: MR. ANDREW C. ERSKINE
219 South Dearborn Street, Suite 500,
Chicago, Illinois 60604
(312)353-5300

For the Defendant:
LAW OFFICES OF VADIM A. GLOZMAN
BY: MR. VADIM A. GLOZMAN
53 West Jackson Boulevard
Suite 1128
Chicago, Illinois 60604
(312) 726-9015

Court Reporter:

CHARLES R. ZANDI, CSR, RPR, FCRR
Official Court Reporter
United States District Court
219 South Dearborn Street, Room 2144-G
Chicago, Illinois 60604
Telephone: (312) 435-5387
email: Charles_zandi@ilnd.uscourts.gov

(Proceedings heard in open court:)

THE CLERK: 18 CR 789, USA versus Mitrovich.

MR. ERSKINE: Good morning, your Honor. Andrew Erskine on behalf of the United States.

MR. GLOZMAN: Good morning, your Honor. Vadim Glozman on behalf of Mr. Mitrovich, who's present to my left.

THE DEFENDANT: Good morning.

THE COURT: Good morning. We're here on a fully-briefed motion to compel. I'm wondering what the government's thoughts are on the matters that were argued in the defendant's reply brief.

MR. ERSKINE: Sure, your Honor. The short response is that -- so, the government disagrees with a lot of the representations of how Tor works within -- not generally speaking, but some of the finer points. But that's kind of neither here nor there, because the sort of system or the series of steps described in the reply brief don't apply to what happened in this case, as sworn to in the affidavit based on information provided by the foreign law enforcement.

And that is this was -- what was described in the reply brief was just talking about how you access different Internet sites, how you were going to stay within the confines of the Tor browser. But as is sort of made plain in the affidavit, you know, as repeated in the government's response, this was a situation where there was a link to download a

video file and then a button -- then a prompt warning the user, here the defendant, that this is going to open up outside of the top -- Tor browser. And I'm paraphrasing. Whatever language is in the response is the language in the response. And then they click that link and proceed and open the thing outside of the Tor browser; and it plays, and it connects over a public connection.

So, that's really not addressed. It's not a matter of going to YouTube and watching videos. We're talking about opening a native file outside of the Tor browser. That's why it's different. That's why this was not addressed at all in the reply.

So, at the end of the day, you still have a situation -- another point I'll make is the question was: Why wouldn't everyone do it this way? Why do the NIT? Why get the warrant if they can just do it this way? And because the answer is -- I'm speculating here. I don't know. I'm speculating, but my belief of what the answer is is that the vast majority of targets, when they see that prompt saying this video is going to take you off of Tor and open you outside of Tor, they wouldn't click that. They'd say, "No, thank you." But in this case, that's not what --

THE COURT: I'm not sure that's what the warning on the link said. The warning just said you're going to go to an external website.

MR. ERSKINE: Exactly.

THE COURT: It doesn't say anything Tor or not Tor. I'm not sure that matters, but as a factual -- if we're going to accurately portray what happened here, the warning wasn't you were going to go off of Tor and your IP address is going to be revealed. That's not what the warning said.

MR. ERSKINE: Absolutely not, no. That's a fair point.

Another distinction I'll draw between the NIT context and this context is that the -- in the NIT frame -- framework, you know, that is an FBI-conducted operation, and the FBI cannot itself distribute child pornography.

So, as was referred to in the reply brief and as is described in the cases, these are situations where people are going to a website and are finding like an error page, you cannot access. And then it was sort of in that situation that, you know, the NIT program has to do its thing to un -- to unveil the public IP address of the target; whereas, again, this is a different context where they are serving up -- the foreign government was serving out the actual child pornography video, linking to it, making it available, and then it opens up; and then through the natural -- not natural, but through the configuration of that video file, just connects over a public IP address.

So, that just -- I say all this in response to the

argument in the reply that it must be the case that they used the NIT approach because nothing else is possible. And I'm doing sort of my best to look at the records and the cases and sort of argue it, and I believe defense counsel is as well; but at the end of the day, I think that the -- the basis for the allegation that it must be, the only explanation is that an NIT was used is just not well-founded.

But what we do know --

THE COURT: I'm not sure you're capturing what the reply brief is actually arguing.

MR. ERSKINE: Okay. Fair enough. But what the --

THE COURT: I mean, the initial motion, the principal, if not exclusive, argument was Mr. Mitrovich was tricked into clicking on the link and didn't voluntarily give up his IP address. And I was skeptical about that argument, although my mind was open.

That argument is not made, at least not at length, in the reply brief. The reply brief, in my mind, completely switches gears and makes another argument, which is malware was used to infect Mr. Mitrovich's computer.

And so let me ask you this: If malware was -- if the law enforcement authorities in Australia had malware put on Mr. Mitrovich's computer when he clicked on that link, would that be a Fourth Amendment search?

MR. ERSKINE: Your Honor, as I stand here, I don't

know.

THE COURT: I think maybe -- and again, I don't know what the answer is, either, but I can see an argument based on *Jones* that putting malware on somebody else's computer is the functional equivalent of a physical trespass, the kind of physical trespass that was at issue in *Jones versus United States*, like putting a GPS monitor on somebody's car.

And again, I don't know whether that analogy holds or not as a matter of Fourth Amendment law, but I can see that argument being made.

But the logically anterior question in order to get to that legal issue is: Was malware put on Mr. Mitrovich's computer? And I didn't hear you address that issue.

MR. ERSKINE: It is my understanding, based on the information that was conveyed by the foreign government, you know, as set forth in the affidavit, that that is not how this works. Malware was not downloaded onto Mr. Mitrovich's computer. It was as simple as set forth in the affidavit.

THE COURT: Okay. What affidavit? Was the affidavit attached to any of the papers? The reason I ask is I have not seen the affidavit because I don't believe it was -- I don't believe it was in the record.

MR. GLOZMAN: I don't believe so, either.

THE COURT: Is it maybe -- is there a criminal complaint in this case that it was attached to?

MR. ERSKINE: It's just the search warrant affidavit. I apologize. It was referenced, I believe, in both the briefs, but I can tender a copy right now.

THE COURT: Do you have a copy?

MR. GLOZMAN: Not with me, but I know what it says.

THE COURT: I don't mean with you now. Have you been given a copy?

MR. GLOZMAN: Yeah. And that's what my factual predicate is based on.

THE COURT: Let me get a copy of this.

(Tendered.)

MR. GLOZMAN: Your Honor, if I may just clear something up, the way I read both that -- and it's not only that. That actually doesn't include everything. There are a number of 302s that talk about additional steps taken. We can tender that to the Court also.

But what happened was the United States was actually using this software. They identified the website TLZ. They knew they couldn't use it, so it actually says in there they gave the software to New Zealand, so the New Zealand government was using a software given them by the United States. They set this up.

Now, the way the Tor network works, your Honor, and I have this in our reply --

THE COURT: If you're arguing as to what happened,

I think it's -- you're saying there was malware put on Mr. Mitrovich's computer. You're saying there wasn't. Any argument on that is going to go in one ear and out the other just because I don't -- I have nothing from the government giving the government its side of the story. I have your side of the story, and I know why you're saying there's malware on Mr. Mitrovich's computer.

MR. GLOZMAN: I understand.

THE COURT: So, I could basically see the government making two arguments in response to your reply brief. The first is even if malware were -- the first would be a legal argument. Even if malware had been placed on Mr. Mitrovich's computer as a means of getting his IP address, it wouldn't matter because that's not a Fourth Amendment search, so we don't even need to have discovery on that.

The second argument, which is an alternative argument, and not mutually exclusive to the first, is a factual one, which is, in point of fact, no malware was placed on Mr. Mitrovich's computer.

All I have are the -- I know you're giving me your best understanding, but we don't really have anything in the record that gives the government's -- that supports the government's view on that perhaps logically anterior question.

MR. ERSKINE: Sure. And, your Honor, I had contemplated asking leave to file a surreply.

MR. GLOZMAN: No objection.

THE COURT: I think that would be best. Because it really was a new argument -- and I'm not being pejorative on that; but it's an argument that was very well developed in the defendant's reply brief, and I don't think you could have anticipated that argument from the motion. So, I think it would be best if I give you a chance to respond to what really is a new argument that's been brought to the table.

How long do you need?

MR. ERSKINE: Your Honor, could I -- just in case I need to reach out to anyone in support of this, could I have three weeks?

THE COURT: Any objection to that?

MR. GLOZMAN: He can have a month if he wants to.

THE COURT: Why don't we say three weeks.

THE CLERK: March 16th.

THE COURT: And then maybe you'll want to -- we could come in either later in the week of the 16th, or I can give you a chance to address the government's submission in writing.

MR. GLOZMAN: Do you want -- if I could suggest maybe do a status date about two weeks after, and if I want to file something, I'll file something in the interim, between when the government files something and the status date.

THE COURT: That's fine. We can come in during the

week of March 30th.

THE CLERK: How about April 1st.

MR. GLOZMAN: That's fine with me.

THE CLERK: 9:45 a.m.

MR. ERSKINE: That works.

THE COURT: So again, just to be clear, it could be -- if you grant his premise, factual premise that there was malware placed on Mr. Mitrovich's computer, maybe that's not a Fourth Amendment search; and then you could say we don't need discovery on whether there was malware because it wouldn't matter because it wasn't a Fourth Amendment search anyway.

And/or, you can argue, "In point of fact, this is how it worked, and there was no malware put on Mr. Mitrovich's computer." And then I have to decide whether the record is clear enough from the papers in front of me that we don't need discovery on that issue. Or maybe there's a third and a fourth argument that you can think of that I'm thinking of.

MR. ERSKINE: Right, sure. And discovery could be something short of the specific things that defense counsel is asking for.

THE COURT: Yeah, maybe.

MR. GLOZMAN: That's fine. At the end of the day if they want to concede there was malware and we have to argue the Fourth Amendment, that's fine, and they don't have to give it over.

THE COURT: Right.

MR. ERSKINE: I'll file something.

THE COURT: We'll see what happens. This is a very interesting issue. I appreciate both sides' briefs. They were both very, very well done, and this is a relatively new and very interesting area of the law, so I appreciate your efforts.

MR. ERSKINE: So, your Honor, the government would move to exclude time through and including the next date, in light of the pending motion.

MR. GLOZMAN: No objection.

THE COURT: Without objection, time is excluded through our next date. Thanks.

MR. ERSKINE: Thank you, your Honor.

THE DEFENDANT: Thank you, your Honor.

(Which were all the proceedings heard.)

CERTIFICATE

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/Charles R. Zandi _____ *February 8, 2023*

Charles R. Zandi
Official Court Reporter

_____
Date